CLAIMS

1. A packet interception system for intercepting message packets transferred over a network, the packet interception system comprising:

A. a processed packet store; and

B. an intercepted packet processor configured to process a currently-intercepted message packet and a hash value generated for a previously-processed message packet in connection with a selected hash algorithm to generate a hash value for the currently-intercepted message packet thereby to generate a processed message packet and to store the processed message packet in the processed packet store.

2. A packet interception system as defined in claim 1 in which one of said currently-intercepted message packet is a first intercepted message packet, the intercepted packet processor being configured to use a selected value along with the first intercepted message packet in generating the processed message packet therefor.

3. A packet interception system as defined in claim 2 in which the selected value includes a session identifier value.

4. A packet interception system as defined in claim 1 in which said intercepted packet processor is further configured to append to each currently-intercepted message packet a time stamp reflective of a time at which the currently-intercepted message packet is received, the time stamp further being used in generating the hash value.

5. A packet interception system as defined in claim 1 in which said intercepted packet processor is further configured to generate, for selected processed message packets, respective digital signatures, and to store each digital signature in the processed packet store with the respective processed message packet for which it was generated.

6. A packet interception system as defined in claim 1 further including an intercept system monitor configured to monitor at least one predetermined aspect of operation of said packet processor, the intercept system monitor communicating with said packet processor over a wireless communication link.

7. A method of processing message packets intercepted over a network, the method comprising the steps of:

A. an intercepted packet processing step in which a currently-intercepted message packet is processed in connection with a hash value generated for a previously-processed message packet using a selected hash algorithm to generate a hash value for the currently-intercepted message packet thereby to generate a processed message packet

B. storing the processed message packet in a processed packet store.

8. A method as defined in claim 7 in which one of said currently-intercepted message packet is a first intercepted message packet, the intercepted packet processing step including a step of using a selected value along with the first intercepted message packet in generating the processed message packet therefor.

9. A method as defined in claim 8 in which the selected value includes a session identifier value.

10. A method as defined in claim 7 in which said intercepted packet processing step includes the step of appending to each currently-intercepted message packet a time stamp reflective of a time at which the currently-intercepted message packet is received, the time stamp further being used in generating the hash value.

11. A method as defined in claim 7 in which said intercepted packet processing step includes the step of generating, for selected processed message packets, respective digital signatures for storage in the processed packet store with the respective processed message packet for which it was generated.

12. A packet verification system for verifying message packets intercepted over a network, the packet verification system comprising:

A. a processed packet store configured to store a header and a series of processed message packets each processed message packet including a message packet and a hash value; and

B. a packet verification processor configured to, in verification of a selected one of said processed message packets in said series, process successive processed message packets prior thereto in the series, for each processed message packet, as a current processed message packet, the packet verification processor being configured to process the message packet of the current processed message packet and a hash value associated with a hash value associated with a previous processed message packet in the series in connection with a selected hash algorithm thereby to generate a hash value for the message packet, compare

the generated hash value to the hash value associated with the current processed message packet and determine whether the message packet is verified based on the comparison.

13. A packet verification system as defined in claim 12 in which one of said current processed message packet is a first intercepted message packet, the verification packet processor being configured to use a selected value along with the first processed message packet in generating the processed message packet therefor.

14. A packet verification system as defined in claim 13 in which the selected value includes a session identifier value.

15. A packet verification system as defined in claim 12 in which said verification packet processor is further configured to process, in connection with each current processed message packet, a time stamp reflective of a time at which the current processed message packet was received, in connection with the hash algorithm.

16. A packet verification system as defined in claim 12 in which said selected ones of said processed message packets further have respective digital signatures, the verification processor further being configured to verify the digital signature associated with each processed message packet to be processed thereby.

17. A packet verification system as defined in claim 1 further including an intercept system monitor configured to monitor at least one predetermined aspect of operation of said packet verification

processor, the intercept system monitor communicating with said packet verification processor over a wireless communication link.

18. A packet verification method for verifying message packets intercepted over a network and stored in a processed packet store configured to store a header and a series of processed message packets each processed message packet including a message packet and a hash value verification of a selected one of said processed message packets in said series, the method comprising the steps of iteratively, up to the selected one of said processed message packets:

A. process, for a current one of said processed message packets, the message packet of the current processed message packet and a hash value associated with a hash value associated with a previous processed message packet in the series in connection with a selected hash algorithm to generate a hash value for the message packet;

B. compare the generated hash value to the hash value associated with the current processed message packet; and

C. determine whether the message packet is verified based on the comparison.

19. A packet verification method as defined in claim 18 in which one of said current processed message packet is a first intercepted message packet, the processor processing step including the step of using a selected value along with the first processed message packet in generating the processed message packet therefor.

20. A packet verification method as defined in claim 19 in which the selected value includes a session identifier value.

21. A packet verification method as defined in claim 18 in which said processing step includes the step of processing, in connection with each current processed message packet, a time stamp reflective of a time at which the current processed message packet was received, in connection with the hash algorithm.

22. A packet verification method as defined in claim 18 in which said selected ones of said processed message packets further have respective digital signatures, the processing step further including the step of verifying the digital signature associated with each processed message packet to be processed thereby.

23. A packet interception system

A. a packet interception device configured to intercept message packets transferred over a network, and

B. an intercept system monitor configured to monitor at least one predetermined aspect of operation of said packet interception device, the intercept system monitor communicating with said packet interception device over a wireless communication link.